Summary

This paper presents a strategy for dynamically monitoring digital controllers in the laboratory for susceptibility to electromagnetic disturbances that compromise control integrity. The integrity of digital control systems operating in harsh electromagnetic environments can be compromised by upsets caused by induced transient electrical signals. Digital system upset is a functional error mode that involves no component damage, can occur simultaneously in all channels of a redundant control computer, and is software dependent. The motivation for this work is the need to develop tools and techniques that can be used in the laboratory to validate and/or certify critical aircraft controllers operating in electromagnetically adverse environments that result from lightning, high-intensity radiated fields (HIRF), and nuclear electromagnetic pulses (NEMP).

The detection strategy presented in this paper provides dynamic monitoring of a given control computer for degraded functional integrity resulting from redundancy management errors, control calculation errors, and control correctness/effectiveness errors. In particular, this paper discusses the use of Kalman filtering, data fusion, and statistical decision theory in monitoring a given digital controller for control calculation errors. The control laws calculated in the digital controller are modeled as linear (or linearized) recursive state equations. This model is used in the design of Kalman filters that estimate the correct control calculations. These estimates of the correct calculations are compared with the calculations obtained by the control computer. Residuals are generated and used in probabilistic decision rules to determine if the calculations performed by the control unit are faulty. A decision is made for the command calculation of each control loop, and these local decisions are optimally weighted and fused into a decision on the integrity of control calculations. A simple example is included to illustrate the concept.

Introduction

Future advanced aircraft will require systems for stability augmentation as well as guidance and control that will be critical to the flight of the aircraft. The trend in avionics technology is the implementation of control laws on digital computers that are interfaced to the sensors and control surface actuators of the aircraft. Since these control systems will be flight critical, the problem of verifying the integrity of the control computer in adverse, as well as nominal, operating environments becomes a key issue in the development and certification of a critical control system.

An operating environment of particular concern results from the presence of electromagnetic fields caused by sources such as lightning, high-intensity radiated fields (HIRF), and nuclear electromagnetic pulses (NEMP). Electromagnetic fields may cause analog electrical transients to be induced on the aircraft wiring, and these signals can propagate to the onboard electronic equipment despite shielding and protective devices such as filters and surge suppressors. Digital computer systems have two types of effects that can be caused by transient electrical signals. The first is component damage that requires repair or replacement of the equipment. The second effect to a digital system is characterized by functional error modes, collectively known as *upset*, which involve no component damage.

Functional error modes of a fault-tolerant controller that can be termed as upset in the system are characterized by (1) faulty input/output (I/O) processing and command calculations that result in off-nominal system behavior or degraded system performance, and (2) faulty redundancy management decisions that result in degraded system performance and/or reliability. In the case of upset, normal operation can be restored to the system by corrective action such as resetting/reloading the software or by an internal recovery mechanism, such as an automatic rollback to a system state prior to the disturbance. The subject of effective and reliable internal upset recovery mechanisms is another current topic for research. The usual features of fault-tolerant systems such as redundant input and output checking and selection, surge suppression devices and filters, and a redundant microprocessor architecture with voting may not be sufficient to ensure correct operation in an electromagnetically adverse operating environment. Surge suppression devices and filters are effective for large-amplitude, high-frequency transients. However, low-amplitude signals at frequencies near the clock speeds of digital circuitry can be generated by electromagnetic fields and propagate to electronic equipment onboard an aircraft. In addition, redundancy protects against single-mode failures that occur in one channel of the system, but it does not protect against the potential common-mode failure (i.e., upset) of all channels in the redundant system as a result of transient signals induced by a single electromagnetic disturbance.

To date, no comprehensive guidelines or criteria exist for detecting upset in fault-tolerant digital control computers, designing reliable internal upset recovery mechanisms, performing tests or analyses on digital controllers to verify control integrity, or evaluating upset susceptibility /reliability in electromagnetically adverse operating environments. In order to assess a digital control computer for upset susceptibility, the issue of upset detection must be addressed. Real-time considerations for upset detection would reduce post data processing requirements during validation/certification testing. Therefore, the objective of this research is to develop an upset detection methodology for real-time laboratory implementation. During laboratory tests, a given digital computer-based control system will be evaluated for upset susceptibility when subjected to analog transient electrical signals like those that would be induced by lightning, HIRF, or NEMP.

The objective of this paper is to present an upset detection strategy for monitoring a given fault-tolerant controller for degraded control integrity resulting from redundancy management errors, control law calculation errors, and control correctness/effectiveness errors. Kalman filtering, statistical decision theory, and data fusion are used in the detection of redundancy management errors and control calculation errors. Analytical redundancy of the control laws provides a reference of the correct control command for the given dynamic mode of the plant. This reference command and an actuator model are used in the control correctness/effectiveness decision. In particular, this paper focuses on the use of Kalman filtering, data fusion, and decision theory in monitoring a digital controller for control law calculation errors.

An upset test methodology for control computers was discussed in reference 1. However, this methodology relies on postprocessing of data collected during each test. Since the detection strategy presented in this paper is for eventual real-time implementation, it will eliminate the need to store data during tests in which upset does not occur. In addition, the strategy provides an indication of where errors occurred for diagnostic purposes so that any desired postprocessing of the data is simplified.

Other works in failure detection methods include the detection of sensor failures in turbofan engines (ref. 2) and the detection of failures in aircraft actuators and control surfaces (ref. 3). In reference 2, analytical redundancy, Kalman filtering, and decision theory were used to detect sensor failures in an F-100 turbofan engine. Out-of-range or large bias errors that occurred instantaneously were detected by comparing measured sensor values with those of an analytical model, taking the absolute value, and comparing this residual to a threshold. Small bias errors and drift in sensor measurements were detected using multiple-hypothesis testing methods in which each hypothesis corresponded to a particular sensor failure. Once a sensor failure was detected, the elements of an interface switch matrix were changed so that a Kalman filter estimate of the sensor value replaced the measurement in the input vector used in the control laws. The methodology of reference 2 was demonstrated on a hybrid real-time simulation of the F-100 engine as well as on a full-scale F-100 engine with good results. However, this methodology was not designed to detect failures in systems with physically redundant sensors and computers and, therefore, does not use data fusion methods.

In reference 3, analytical redundancy and decision theory were used to detect actuator failures and control surface failures in aircraft. The design methodology consisted of two failure detection and identification (FDI) algorithms or subsystems—one for actuator failures and one for control surface failures. In the actuator FDI subsystem, an analytical model was implemented to generate a prediction of the dynamic behavior of the actuators. This prediction was compared with measurements taken from the actuators, and a residual was generated and used in a decision process. The control surface FDI subsystem was designed in a similar fashion. The methodology of reference 3 was demonstrated using a six-degree-of-freedom nonlinear simulation of a modified Boeing 737 airplane with good results. This methodology was not designed to detect failures in physically redundant systems and did not use data fusion techniques.

A formulation of the problem considered in this paper follows a list of symbols used in the notation. The monitoring strategy is presented in the next section and focuses on the detection of control law calculation errors in redundant processors. An example is presented in which the calculation error-detection scheme is demonstrated on a hypothetical quad-redundant processing system. The final section of this paper contains some remarks on the detection strategy.

Symbols

Bold type denotes vector and matrix variables. A dot over a symbol indicates a derivative with respect to time.

$\mathbf{A}$	plant system matrix
$\mathbf{B}$	plant control input matrix
$\mathbf{C}_f^{\gamma}$	system matrix for γ sensors measuring parameter f
$\mathbf{D}_f$	plant state measurement matrix
$d(k)$	global upset decision that results from fusion of $d_c(k)$, $d_e(k)$, and $d_r(k)$
$\mathbf{d}_c^i(k)$	decision vector for control law calculations of processor i
$d_c(k)$	decision scalar for control law calculations that result from fusion of elements in $\mathbf{d}_c^i(k)$
$\mathbf{d}_e(k)$	decision vector for control correctness/effectiveness
$d_e(k)$	decision scalar for control correctness/effectiveness that results from fusion of elements in $\mathbf{d}_e(k)$
$\mathbf{d}_{\text{in}}^i(k)$	decision vector for input selection process of processor i
$\mathbf{d}_{\text{out}}(k)$	decision vector for output selection process of controller
$d_r(k)$	decision scalar for input/output redundancy management that results from fusion of elements in $\mathbf{d}_{\text{in}}^i(k)$ and $\mathbf{d}_{\text{out}}(k)$
$\mathbf{E}_f^i$	input-selection state transition matrix for parameter f of processor i
$\mathbf{F}_c^i$	control law calculation state transition matrix
$\mathbf{G}_c^i$	input matrix for control law calculation state vector of processor i
$\mathbf{H}_c^i$	control law calculation measurement matrix
$\mathbf{I}$	identity matrix
$\mathbf{J}^i$	input-selection state measurement matrix
$\mathbf{K}_c^i(k)$	Kalman filter gain matrix for state estimate for control law
k	discrete time variable
$\mathbf{L}j(k)$	output-selection state transition matrix for jth control law calculation
$\mathbf{M}$	output-selection measurement matrix

$\mathbf{P}$	actuator measurement matrix
$\mathbf{P}_c^i(k\|k-1)$	predicted error covariance matrix for estimate of control law calculation of processor i
$\mathbf{P}_c^i(k\|k)$	updated error covariance matrix for estimate of control law calculation of processor i
$\mathbf{Q}_c^i$	covariance matrix for process noise of control law calculation of processor i
$\mathbf{R}_c^i$	covariance matrix for measurement noise of control law calculation of processor i
$\mathbf{r}_c^i(k)$	residual vector of decision rule for detecting control law calculation errors in processor i
$\mathbf{S}_f(k)$	discretized redundant plant sensor vectors for parameter f
$\mathbf{S}_f(t)$	continuous redundant plant sensor vectors for parameter f
$\mathbf{s}_f^\gamma(t)$	γ-redundant sensor measurement of plant parameter f
$\mathbf{T}$	actuator state transition matrix
$u(t)$	control input to plant from actuators
$\mathbf{v}_c^i(k)$	measurement noise for control law calculation of processor i
$\mathbf{v}_f(k)$	measurement noise for redundant sensors of plant parameter f
$\mathbf{v}_{\text{in}}^i(k)$	measurement noise for selected input vector of processor i
$\mathbf{v}_{\text{out}}(k)$	measurement noise for selected output vector of controller
$\mathbf{v}_u(k)$	measurement noise for actuators
$\mathbf{w}_c^i(k)$	process noise for control law calculation of processor i
$\mathbf{w}_f^\gamma(k)$	process noise for γ-redundant sensors measuring plant parameter f
$\mathbf{w}_{\text{in}_f}^i(k)$	process noise for selection of input parameter f of processor i
$\mathbf{w}_{\text{out}_j}(k)$	process noise for selection of control output parameter j
$\mathbf{w}_u(k)$	process noise for actuators
$\mathbf{x}_p(t)$	plant state vector
$\mathbf{x}_c^i(k)$	control law calculation state vector of processor i
$\hat{\mathbf{x}}_c^i(k\|k-1)$	predicted state estimate of control law calculation state vector of processor i
$\hat{\mathbf{x}}_c^i(k\|k)$	updated state estimate of control law calculation state vector of processor i
$\mathbf{Y}_{\text{in}}^i(k)$	selected input vector for processor i
$\mathbf{Y}_{\text{out}}(k)$	selected control output vector of controller
$\mathbf{Y}_{\text{out}}(t)$	continuous form of selected control output vector
$y_{\text{in}_f}^i(k)$	selected value of input parameter f for processor i
$y_{\text{out}_j}(k)$	selected value of control law calculation j
$\mathbf{\Gamma}_j$	noise matrix for output selection process of controller

$\boldsymbol{\zeta}_c^i$	process noise matrix for control law calculation of processor i
$\boldsymbol{\Lambda}$	selected-output vector compression matrix
$\boldsymbol{\xi}_f^\gamma$	process noise matrix for γ-redundant sensors of plant parameter f
$\boldsymbol{\rho}$	process noise matrix for actuators
$\boldsymbol{\phi}$	process noise matrix for plant
$\boldsymbol{\psi}_f^i$	noise matrix for input selection process of plant parameter f of processor i
$\boldsymbol{\Omega}$	plant state measurement matrix

Special notation:

$H0_c$	hypothesis that control law calculation in controller is correct
$H0_c^i$	hypothesis that control law calculations of processor i are correct
$H0_{c_j}^i$	hypothesis that control law calculation j of processor i is correct
$H1_c$	hypothesis that calculation of control laws in controller is incorrect
$H1_c^i$	hypothesis that control law calculations of processor i are incorrect
$H1_{c_j}^i$	hypothesis that control law calculation j of processor i is incorrect
ln	natural logarithm
$P(D0_{c_j}^i \vert H1_{c_j}^i)$	probability of deciding that control law calculation j of processor i is correct given that it is incorrect
$P(D1_{c_j}^i \vert H0_{c_j}^i)$	probability of deciding that control law calculation j of processor i is incorrect given that it is correct
$P(H0_{c_j})$	*a priori* probability that hypothesis $H0_{c_j}^i$ is correct for all processors
$Pfa_{c_j}^i$	probability of a false alarm for control law calculation j of processor i
$Pm_{c_j}^i$	probability of a missed detection for control law calculation j of processor i
PF_c	probability of a false alarm for control law calculations of controller
PF_c^i	probability of a false alarm for control law calculations of processor i
PM_c	probability of a missed detection for control law calculations of controller
PM_c^i	probability of missed detection for control law calculations of processor i
R	set of real numbers
T	matrix transpose
$\in$	is an element of
$\mu_{c_j}^i$	mean of innovations sequence for control law calculation j of processor i

Subscripts:

c	control law calculation variable
e	command correctness/effectiveness variable
f	sensor variable for plant parameter f
in	input variable

out	output variable
p	plant variable
r	input/output redundancy management variable
u	actuator variable

Subsubscripts:

f	index for plant parameter
j	index for control law calculations

Superscripts:

i	index for redundant processors
m	number of plant parameters being measured
N	dimension of actuator output state space
n	dimension of control law calculation state space
p	dimension of plant state space
γ	index for redundant sensors
δ_f	number of redundant sensors measuring plant parameter f
η	dimension of control output space
σ	number of redundant processors
-1	matrix inverse

Abbreviations:

A/D	analog to digital
calc.	calculation
cmd.	command
cntl.	control
cond.	conditioning
decis.	decision
effect.	effectiveness
D/A	digital to analog
EM	electromagnetic
FDI	failure detection and identification
HIRF	high-intensity radiated fields
I/O	input/output
meas.	measurement
mgt.	management
NEMP	nuclear electromagnetic pulse
$\mu\mathrm{P}_1$, $\mu\mathrm{P}_2$, ..., $\mu\mathrm{P}_\sigma$	microprocessors

ROC	Receiver Operating Characteristics
redun.	redundancy
S/H	sample and hold
sig.	signal

Problem Formulation

The fault-tolerant controller to be evaluated for upset susceptibility is interfaced in the laboratory to a simulation of the plant, redundant sensors, and actuators so that closed-loop dynamics are represented during testing. A block diagram of the laboratory setup is shown in figure 1. The controller with σ processors (or microprocessors (μP), designated as μP_1 to μP_σ) is subjected to disturbances like those that can occur in an electromagnetically harsh environment. In the case of lightning, transient signals that would be induced on internal wiring are generated. In the case of HIRF, electromagnetic (EM) fields that could occur from radars or high-power radio transmitters are generated. The control system is dynamically monitored for upset in real-time testing. In the event of the occurrence of upset during testing, the detection methodology will provide a framework for diagnosis of the upset in the given digital controller.

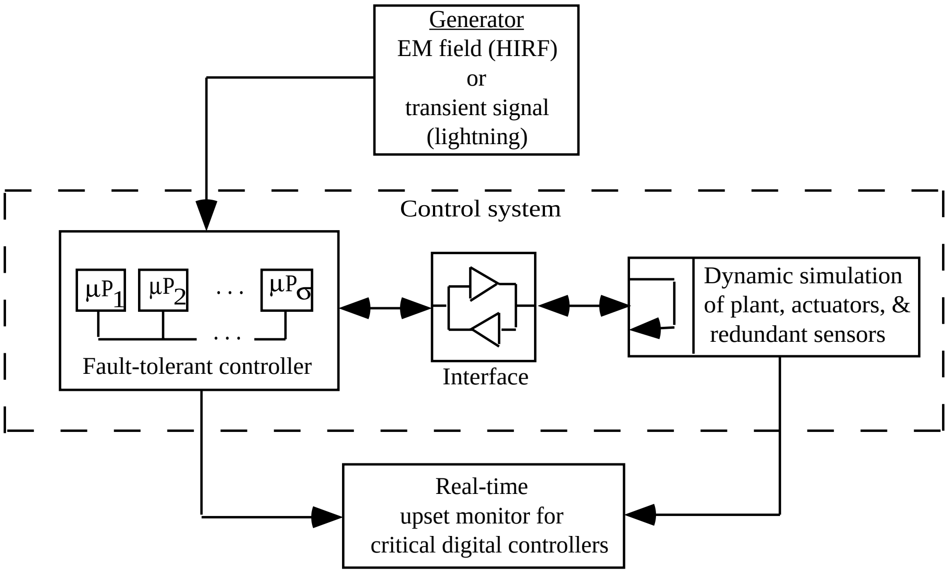

Figure 1. Laboratory configuration for upset evaluation of digital controllers.

Consider the block diagram shown in figure 2 of a given control system consisting of the plant, redundant sensors, actuators, and fault-tolerant control computer. Input/output conversions and signal conditioning between the plant and controller are represented by the indicated blocks. Input processing functions including analog-to-digital (A/D) conversion, frequency-to-digital conversion, surge suppressors for protection against high-level transient signals, and filters to reduce high-frequency noise have been represented by the A/D and signal conditioning block. Output processing functions such as signal conditioning and digital-to-analog (D/A) conversion are represented by the D/A and signal conditioning block.

The given fault-tolerant controller is modeled to consist of three basic blocks. The input selection and redundancy management block performs rate and/or range checks of the data values and generates the input data vector for each of the microprocessors. The redundant microprocessors calculate the control commands based on the input vector for each processor. Redundancy in the control computer protects against single-mode failure of components during normal operation.

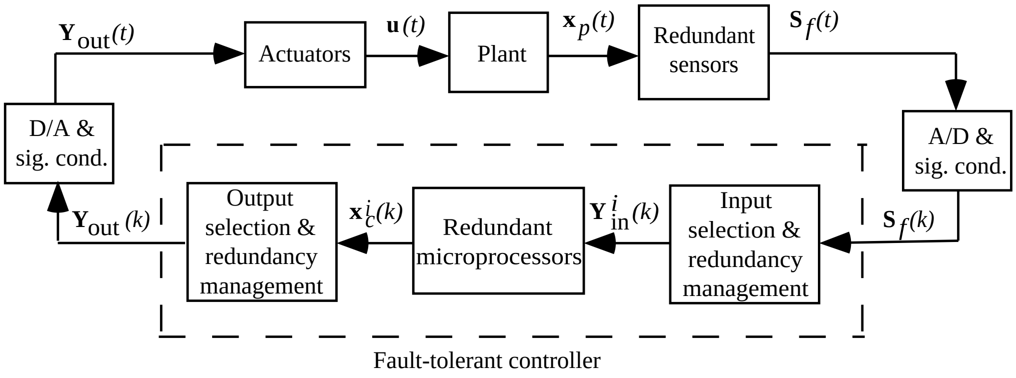
$\mathbf{Y}_{\text{out}}(t)$
Actuators
$\mathbf{u}(t)$
Plant
$\mathbf{x}_p(t)$
Redundant sensors
$\mathbf{S}_f(t)$
D/A & sig. cond.
A/D & sig. cond.
$\mathbf{Y}_{\text{out}}(k)$
Output selection & redundancy management
$\mathbf{x}_c^i(k)$
Redundant microprocessors
$\mathbf{Y}_{\text{in}}^i(k)$
Input selection & redundancy management
$\mathbf{S}_f(k)$
Fault-tolerant controller

Figure 2. Control system with redundant sensors and microprocessors.

The output selection and redundancy management block performs rate and/or range checks on the calculated commands from each processor and determines via voting, or some other scheme, the command to be output from the controller for each control loop.

The linear model in the following discussion is proposed for the given control system of figure 2. The number of redundant sensors for the measurement of the fth plant parameter is given as δ_f, and the number of different plant measurements is given by m. The number of redundant processors is designated by σ. Each processor performs n calculations. The number of control outputs is given by η. The control action in the plant is effected by N actuator signals. In equations (1) through (6), state variables, sensor values, and input/output variables are designated by x, s, and y, respectively. Control inputs are designated by u. System noise processes are designated by w. Variable superscripts index replicates of redundant system elements. Subscripts characterize the variables, and subsubscripts index elements of vector variables. Bold type denotes vector and matrix variables.

In the linear model the plant state vector is given as

$$\dot{\mathbf{x}}_p(t) = \mathbf{A}\,\mathbf{x}_p(t) + \mathbf{B}\,\mathbf{u}(t) + \boldsymbol{\phi}\,\mathbf{w}_p(t) \qquad (\mathbf{x}_p(t) \in R^p) \qquad (1)$$

with sensors

$$\mathbf{S}_f(t) = \left[s_f^1(t)\ s_f^2(t)\ \ldots\ s_f^{\delta_f}(t)\right]^T \qquad (\mathbf{S}_f(t) \in R^{\delta_f})$$

where

$$s_f^\gamma(t) = \mathbf{C}_f^\gamma\ \mathbf{x}_p(t) + \boldsymbol{\xi}_f^\gamma\ \mathbf{w}_f^\gamma(t) \qquad \left(\gamma = 1, 2,\ \ldots,\ \delta_f; f = 1, 2,\ \ldots,\ m; s_f^\gamma(t) \in R\right) \qquad (2)$$

For input selection and redundancy management,

$$\mathbf{Y}_{\text{in}}^i(k) = [y_{\text{in}_1}^i(k)\ y_{\text{in}_2}^i(k)\ \ldots\ y_{\text{in}_m}^i(k)]^T \qquad (\mathbf{Y}_{\text{in}}^i(k) \in R^m)$$

with

$$y_{\text{in}_f}^i(k) = \mathbf{E}_f^i(k)\ \mathbf{S}_f(k) + \psi_f^i\ \mathbf{w}_{\text{in}_f}^i(k) \qquad \left(i = 1, 2,\ \ldots,\ \sigma; y_{\text{in}_f}^i(k) \in R; \mathbf{S}_f(k) \in R^{\delta_f}\right) \qquad (3)$$

where

$$\mathbf{S}_f(k) = [s_f^1(k)\ s_f^2(k)\ \ldots\ s_f^{\delta_f}(k)]^T \qquad (f = 1, 2,\ \ldots,\ m)$$

For control law calculations of redundant controllers,

$$\mathbf{x}_c^i(k+1) = \mathbf{F}_c^i\ \mathbf{x}_c^i(k) + \mathbf{G}_c^i\ \mathbf{Y}_{\text{in}}^i(k) + \boldsymbol{\zeta}_c^i\ \mathbf{w}_c^i(k) \qquad (i = 1, 2,\ \ldots,\ \sigma; \mathbf{x}_c^i(k) \in R^n) \qquad (4)$$

where

$$\mathbf{x}_c^i(k) = [x_{c_1}^i(k)\ x_{c_2}^i(k)\ \ldots\ x_{c_n}^i(k)]^T \qquad (x_{c_j}^i(k) \in R)$$

For output processing and redundancy management,

$$\mathbf{Y}_{\text{out}}(k) = \mathbf{\Lambda}[y_{\text{out}_1}(k)\ y_{\text{out}_2}(k)\ \ldots\ y_{\text{out}_n}(k)]^T \qquad (\mathbf{Y}_{\text{out}}(k) \in R^{\eta} = +1)$$

$$y_{\text{out}_j}(k) = \mathbf{L}_j(k)\ \mathbf{x}_{c_j}(k) + \mathbf{\Gamma}_j\ \mathbf{w}_{\text{out}_j}(k) \qquad (j = 1, 2,\ \ldots,\ n; y_{\text{out}_j}(k) \in R) \tag{5}$$

where

$$\mathbf{x}_{c_j} = [x_{c_j}^1(k)\ x_{c_j}^2(k)\ \ldots\ x_{c_j}^{\sigma}(k)]^T \qquad (\mathbf{x}_{c_j}(k) \in R^{\sigma})$$

For the actuators,

$$\mathbf{u}(t) = \mathbf{T}\ \mathbf{Y}_{\text{out}}(t) + \rho\ \mathbf{w}_u(t) \qquad (\mathbf{u}(t) \in R^N) \tag{6}$$

where

$$\mathbf{Y}_{\text{out}}(t) = [Y_{\text{out}_1}(t)\ Y_{\text{out}_2}(t)\ \ldots\ Y_{\text{out}_\eta}(t)]^T \qquad (\mathbf{Y}_{\text{out}}(t) \in R^{\eta})$$

Equations (1)–(6) represent a hybrid model of continuous-time and discrete-time components. Equation (1) is the continuous-time state equation for the plant. Matrix $\mathbf{A}$ is the plant system matrix, $\mathbf{u}(t)$ is the control input, and $\mathbf{w}_p(t)$ reflects noise and/or modeling errors. Equation (2) is the continuous-time sensor model for the redundant sensors with $\mathbf{w}_{s_f}^i(t)$ representing the sensor noise. Equation (3) is the discrete-time model for the selection and management of redundant sensor inputs $\mathbf{S}_{p_f}(k)$ for the fth plant parameter measurement with the noise term $\mathbf{w}_{\text{in}_f}^i(k)$ representing modeling error. Matrix $\mathbf{E}_f^i(k)$ is time varying to represent selection, rejection, voting, or fusion of redundant sensor measurements. If the given system has an input data selection process without data fusion, the elements of $\mathbf{E}_f^i(k)$ will be 0 or 1 and may be based on heuristics, such as the result of range and/or rate checks on the sensor measurements. In systems that fuse sensor measurements into a single value, matrix $\mathbf{E}_f^i(k)$ would represent the input data fusion process. Equation (4) is the discrete-time state equation for the calculation vector of the ith processor, and matrix $\mathbf{F}_c^i$ is the transition matrix. Matrix $\mathbf{G}_c^i$ is the measurement matrix for measurement vector $\mathbf{Y}_{\text{in}}^i(k)$ of the ith processor. Term $\mathbf{w}_c^i(k)$ reflects noise and/or modeling errors associated with the calculation vector from the ith processor. Equation (5) is the discrete-time model for the selection and management of the redundant calculations with modeling error accounted for in the noise term $\mathbf{w}_{\text{out}_j}(k)$. Matrix $\mathbf{L}_j(k)$ is time varying to represent selection or fusion of calculations for the output $y_{\text{out}_j}(k)$ of the jth calculation during operation of the system. If the given system has a voting strategy for calculations, the elements of $\mathbf{L}_j(k)$ will be 0 or 1 and may be based on heuristics associated with the voting strategy. In systems that combine calculations into one output, $\mathbf{L}_j(k)$ would represent the calculation fusion process. Vector $\mathbf{Y}_{\text{out}}(k)$ represents the output control calculations. Matrix $\mathbf{\Lambda}$ collapses the calculation vector into the output command vector. Equation (6) is the continuous-time actuator model. The actuators receive the command vector $\mathbf{Y}_{\text{out}}(t)$ and affect the dynamics of the plant via $\mathbf{u}(t)$. The term $\mathbf{w}_u(t)$ reflects noise and/or modeling errors.

Monitoring Strategy for Fault-Tolerant Control System

In order to detect redundancy management errors, control calculation errors, and control effectiveness errors in the fault-tolerant controller, measurements of the control system of figure 2

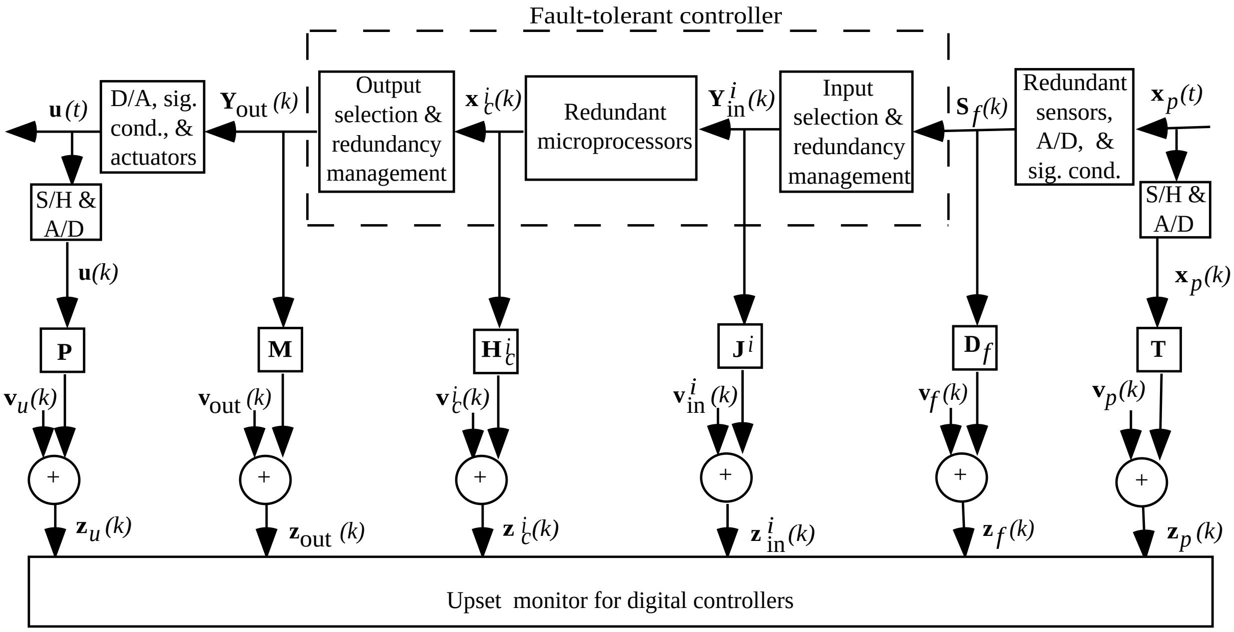

Figure 3. Fault-tolerant controller measurements.

must be taken by the monitor. These measurements are indicated in figure 3, and their equations are presented as follows.

The measurement of the plant state is given by

$$\mathbf{z}_p(k) = \mathbf{\Omega}\ \mathbf{x}_p(k) + \mathbf{v}_p(k) \qquad (\mathbf{z}_p(k) \in R^p) \tag{7}$$

The measurement of sensor outputs is given by

$$\mathbf{z}_f(k) = \mathbf{D}_f\ \mathbf{S}_f(k) + \mathbf{v}_f(k) \qquad \left(f = 1, 2,\ \ldots,\ m; \mathbf{z}_f(k) \in R^{\delta_f}\right) \tag{8}$$

The measurement of input vectors is given by

$$\mathbf{z}_{\mathrm{in}}^i(k) = \mathbf{J}^i\ \mathbf{Y}_{\mathrm{in}}^i(k) + \mathbf{v}_{\mathrm{in}}^i(k) \qquad (\mathbf{z}_{\mathrm{in}}^i(k) \in R^m) \tag{9}$$

The measurement of calculated commands is given by

$$\mathbf{z}_c^i(k) = \mathbf{H}_c^i\ \mathbf{x}_c^i(k) + \mathbf{v}_c^i(k) \qquad (j = 1, 2,\ \ldots,\ n; \mathbf{z}_c^i(k) \in R^n) \tag{10}$$

The measurement of the output command vector is given by

$$\mathbf{z}_{\mathrm{out}}(k) = \mathbf{M}\ \mathbf{Y}_{\mathrm{out}}(k) + \mathbf{v}_{\mathrm{out}}(k) \qquad (\mathbf{z}_{\mathrm{out}}(k) \in R^\eta) \tag{11}$$

and the measurement of the actuator is given by

$$\mathbf{z}_u(k) = \mathbf{P}\ \mathbf{u}(k) + \mathbf{v}_u(k) \qquad (\mathbf{z}_u(k) \in R^N) \tag{12}$$

In equations (7)–(12), $\mathbf{\Omega}$, $\mathbf{D}_f$, $\mathbf{J}^i$, $\mathbf{H}_c^i$, $\mathbf{M}$, and $\mathbf{P}$ are the measurement matrices. The terms $\mathbf{v}_p(k)$, $\mathbf{v}_f(k)$, $\mathbf{v}_{\mathrm{in}}^i(k)$, $\mathbf{v}_c^i(k)$, $\mathbf{v}_{\mathrm{out}}(k)$, and $\mathbf{v}_u(k)$ represent measurement noise. All noise processes in equations (1)–(12) are assumed to be independent, white, and Gaussian.

The fault-tolerant control computer is monitored for errors in redundancy management and control command calculations, as well as for command correctness/effectiveness given the dynamic mode of the plant. In the context of this mathematical formulation, upset is defined as a change in any of the matrices $\mathbf{E}_f^i(k)$ of equation (3), $\mathbf{F}_c^i$ and $\mathbf{G}_c^i$ of equation (4), and $\mathbf{L}_j(k)$ of equation (5) that causes a reduction in effectiveness and/or reliability of the control system. A concept for upset detection in digital control computers is presented in figure 4. The upset detection strategy has three modules to monitor for input/output redundancy management errors, control law calculation errors, and control command errors. The distinction between these last two types of errors should be noted. Control calculation errors result when basic mathematical operations are performed incorrectly by the processor. Control command errors result when incorrect input parameters are used in calculations or when rate/range checks are performed incorrectly on the calculated result. A basic description of the three modules is given, but the paper focuses on the detection of control law calculation errors.

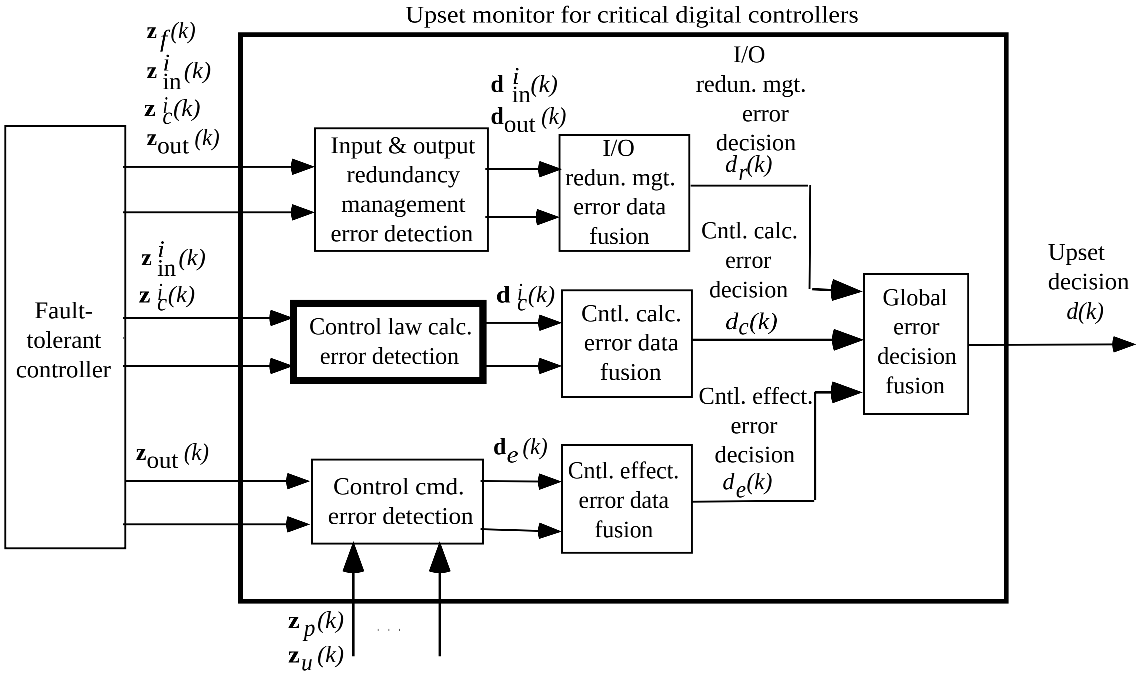
Upset monitor for critical digital controllers
$\mathbf{z}_f(k)$
$\mathbf{z}_{\mathrm{in}}^i(k)$
$\mathbf{z}_c^i(k)$
$\mathbf{z}_{\mathrm{out}}(k)$
Fault-tolerant controller
Input & output redundancy management error detection
$\mathbf{d}_{\mathrm{in}}^i(k)$
$\mathbf{d}_{\mathrm{out}}(k)$
I/O redun. mgt. error data fusion
I/O redun. mgt. error decision
$d_r(k)$
$\mathbf{z}_{\mathrm{in}}^i(k)$
$\mathbf{z}_c^i(k)$
Control law calc. error detection
$\mathbf{d}_c^i(k)$
Cntl. calc. error data fusion
Cntl. calc. error decision
$d_c(k)$
Global error decision fusion
Upset decision
$d(k)$
$\mathbf{z}_{\mathrm{out}}(k)$
Control cmd. error detection
$\mathbf{d}_e(k)$
Cntl. effect. error data fusion
Cntl. effect. error decision
$d_e(k)$
$\mathbf{z}_p(k)$
$\mathbf{z}_u(k)$
. . .

Figure 4. Upset detection concept for digital control systems.

Redundancy management processes in the control computer to be monitored are the input-parameter selection process, the output-command selection process, and the management of redundant resources. An example of a redundancy management error is the computer deciding that one of the redundant sensors is faulty and ignoring its measurements when, in fact, it is operating correctly. Since eliminating an unfaulted sensor reduces the redundancy and overall reliability of the system, this redundancy management error would constitute an upset. The redundancy management monitor detects incorrect changes in the matrices $\mathbf{E}_f^i(k)$ and $\mathbf{L}_j(k)$ of equations (3) and (5), respectively. Elements of these matrices are compared with the input/output selection codes of the controller to determine if the controller has eliminated resources that are not faulty. Input/output selection codes are binary words that are generated by the controller to reflect the choices made by the input/output selection logic.

Inputs to the input selection error detection portion of this monitor are measurements of the sensor outputs ($\mathbf{z}_f(k)$) and measurements of the selected input vector for each channel ($\mathbf{z}_{\mathrm{in}}^i(k)$). If an error is not detected in the input selection process, then each decision variable in the vector $\mathbf{d}_{\mathrm{in}}^i(k)$

will maintain its nominal value of -1. If an error is detected in the input selection process, the corresponding element value of $\mathbf{d}_{\text{in}}^{i}(k)$ becomes unity. Inputs to the output selection error detection part of this monitor are measurements of the calculated control commands ($\mathbf{z}_{c}^{i}(k)$) and the selected output commands ($\mathbf{z}_{\text{out}}(k)$). If an error is not detected in the output selection process, the decision variables in the vector $\mathbf{d}_{\text{out}}(k)$ will maintain a nominal value of -1. If an error is detected in the output selection process, the appropriate element value of $\mathbf{d}_{\text{out}}(k)$ becomes unity. Individual decisions in $\mathbf{d}_{\text{in}}^{i}(k)$ and $\mathbf{d}_{\text{out}}(k)$ are combined or fused into a decision scalar for redundancy management errors ($d_r(k)$).

The control law calculations of each processor are also monitored for errors. This monitoring is done dynamically as the calculations are made. Changes in the matrices $\mathbf{F}_{c}^{i}$ and $\mathbf{G}_{c}^{i}$ of equation (4) are detected by monitoring for errors in the calculated control commands. Inputs to the control law calculation error detector are measurements of the selected input vector for each channel ($\mathbf{z}_{\text{in}}^{i}(k)$) and the calculation vector of each channel ($\mathbf{z}_{c}^{i}(k)$). Individual decisions ($\mathbf{d}_{c}^{i}(k)$) are made for the control law calculations of each processor, and these decisions are fused into a scalar error decision ($d_c(k)$) for the control law calculations of the controller.

Analytical redundancy of the control laws provides a reference of the correct control command for the given dynamic mode of the plant. Inputs to the analytical model of the control laws are measurements of the plant state ($\mathbf{z}_p(k)$). This analytical reference and the actuator measurement $\mathbf{z}_u(k)$) are used in a decision process to determine if the calculated command output vector ($\mathbf{Y}_{\text{out}}(k)$) is correct and is, therefore, effective in regulating the plant under a given dynamic situation. It should be noted that this is not an evaluation of the control law design. The control laws are assumed to be designed appropriately, to be validated prior to this assessment of the controller, and to be effective in controlling the plant. Any lack of effectiveness in the control commands that are output by the controller during this assessment will, therefore, be the result of incorrectness of the commands that could be attributed to incorrectly selected input values or faulty rate/range checks. Thus, considerations such as range and rate limitations of the actuators will be inherent in this evaluation of the effectiveness of the control output. If an error in the control command is not detected, each of the decision variables in the vector $\mathbf{d}_e(k)$ will maintain its nominal value of -1. If an error in control correctness is detected, the appropriate value of $\mathbf{d}_e(k)$ becomes unity. Individual control error decisions are made for each control loop, and these decisions are combined or fused into one scalar error decision ($d_e(k)$) for the correctness/effectiveness of the control output vector.

The decisions corresponding to redundancy management errors, control law calculation errors, and control correctness/effectiveness errors are fused into one global upset decision ($d(k)$), which has a nominal value of -1 and a value of unity for the upset decision. This global fusion process may be a logical OR rule, or it may provide weightings corresponding to the relative costs of the three error processes. In tests during which upset occurs and is signaled by the unity value of $d(k)$, the redundancy management error decisions $\mathbf{d}_{\text{in}}^{i}(k)$ and $\mathbf{d}_{\text{out}}(k)$, the control law calculation error decisions $\mathbf{d}_{c}^{i}(k)$, and the control correctness/effectiveness error decisions $\mathbf{d}_e(k)$ are all stored in the monitor as a diagnostic aid for posttesting data analysis. A strategy for monitoring the control computer for erroneous control law calculations is now presented.

Monitor for Control Law Calculation Error

The approach for monitoring control law calculation errors in a controller with a single processor is shown in figure 5. Since the controller has a single processor, the redundancy index i is unity. The control law calculations are represented as a linear or linearized recursive state equation with state vector $\mathbf{x}_{c}^{i}(k)$. A Kalman filter is used to generate the estimate vector $\widehat{\mathbf{x}}_{c}^{i}(k)$ of the correct state for the calculations based on measurements $\mathbf{z}_{\text{in}}^{i}(k)$ of the selected input vector and measurements $\mathbf{z}_{c}^{i}(k)$ of the control law calculation state vector. The estimate $\widehat{\mathbf{x}}_{c}^{i}(k)$ is compared with the measurement $\mathbf{z}_{c}^{i}(k)$ of the calculation vector to generate a residual vector $\mathbf{r}_{c}^{i}(k)$. A statistical decision rule is then

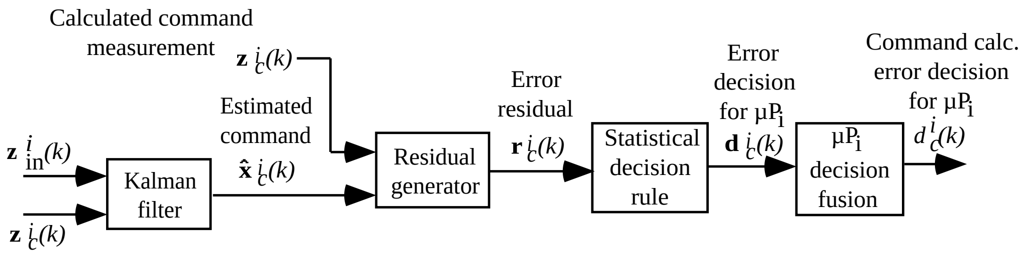

Figure 5. Strategy for monitoring control law calculation errors in digital controllers with a single processor.

applied to each element of the residual vector, and a decision $\mathbf{d}^i_c(k)$ is made regarding the correctness of the calculations, given the selected input vector. Decisions for the individual calculations are then fused into a single decision $(d^i_c(k))$ for the correctness of the calculations.

The approach shown in figure 5 is readily extended to dynamically monitor processor calculations in redundant systems and is illustrated in figure 6. The global decision $d_c(k)$ on whether calculation errors have occurred is based on the fusion of the scalar calculation-error decisions $d^i_c(k)$ for σ processors. The scalar calculation-error decision $d^i_c(k)$ for each processor is generated by the process described in figure 5. Previous work (ref. 4) compared two distributed detection strategies, each using a different type of data fusion. One strategy involved a single global decision based on the fusion of local estimates, and the other strategy involved the fusion of local decisions into a single global decision. The performance of a statistical decision process is determined by the Receiver Operating Characteristics (ROC) curve which is a plot of the probability of detection versus the probability of false alarm, with the decision threshold as the varying parameter. The ROC curve of the strategy with decision fusion was shown to be more desirable for two cases. Therefore, the strategy of figure 6 uses fusion of local decisions. In order to illustrate the strategy for dynamically monitoring the calculations of redundant processors, a simple example is presented.

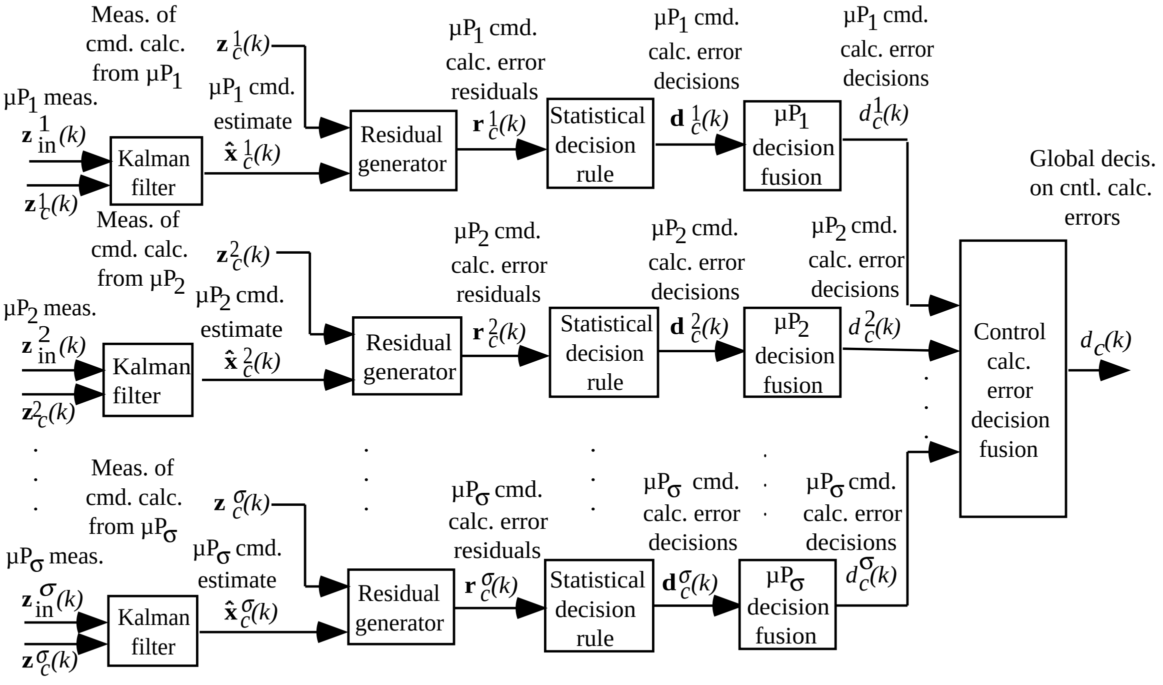
Meas. of cmd. calc. from μP$_1$
z $^1_c(k)$
μP$_1$ meas.
z $^1_{in}(k)$
z $^1_c(k)$
Kalman filter
μP$_1$ cmd. estimate
x̂ $^1_c(k)$
Residual generator
μP$_1$ cmd. calc. error residuals
r $^1_c(k)$
Statistical decision rule
μP$_1$ cmd. calc. error decisions
d $^1_c(k)$
μP$_1$ decision fusion
μP$_1$ cmd. calc. error decisions
$d^1_c(k)$
Meas. of cmd. calc. from μP$_2$
z $^2_c(k)$
μP$_2$ meas.
z $^2_{in}(k)$
z $^2_c(k)$
Kalman filter
μP$_2$ cmd. estimate
x̂ $^2_c(k)$
Residual generator
μP$_2$ cmd. calc. error residuals
r $^2_c(k)$
Statistical decision rule
μP$_2$ cmd. calc. error decisions
d $^2_c(k)$
μP$_2$ decision fusion
μP$_2$ cmd. calc. error decisions
$d^2_c(k)$
Meas. of cmd. calc. from μP$_\sigma$
z $^\sigma_c(k)$
μP$_\sigma$ meas.
z $^\sigma_{in}(k)$
z $^\sigma_c(k)$
Kalman filter
μP$_\sigma$ cmd. estimate
x̂ $^\sigma_c(k)$
Residual generator
μP$_\sigma$ cmd. calc. error residuals
r $^\sigma_c(k)$
Statistical decision rule
μP$_\sigma$ cmd. calc. error decisions
d $^\sigma_c(k)$
μP$_\sigma$ decision fusion
μP$_\sigma$ cmd. calc. error decisions
$d^\sigma_c(k)$
Global decis. on cntl. calc. errors
Control calc. error decision fusion
$d_c(k)$

Figure 6. Strategy for monitoring control law calculation errors in digital controllers with redundant processors.

Example for Quad-Redundant Processor

Consider a system of four redundant processing channels. Let the model of the calculations to be made by the four channels be given by third-order linear recursive equations. Thus, for a processor calculation we have

$$\mathbf{x}_c^i(k+1) = \mathbf{F}_c^i\ \mathbf{x}_c^i(k) + \mathbf{G}_c^i\ \mathbf{Y}_{\text{in}}^i(k) + \zeta_c^i\ \mathbf{w}_c^i(k) \qquad (i = 1, 2, 3, 4) \qquad (13)$$

with a measurement

$$\mathbf{z}_c^i(k) = \mathbf{H}_c^i\ \mathbf{x}_c^i(k) + \mathbf{v}_c^i(k) \qquad (i = 1, 2, 3, 4) \qquad (14)$$

where

$$\mathbf{F}_c^1 = \begin{bmatrix} 0.75 & 1.0 & 0.5 \\ 0 & 0.3 & 1.0 \\ 0 & 0 & 0.5 \end{bmatrix} \quad \mathbf{F}_c^2 = \begin{bmatrix} 0.8 & 0.9 & 0.6 \\ 0 & 0.4 & 0.9 \\ 0 & 0 & 0.5 \end{bmatrix} \quad \mathbf{F}_c^3 = \begin{bmatrix} 0.7 & 0.9 & 0.7 \\ 0 & 0.3 & 0.8 \\ 0 & 0 & 0.4 \end{bmatrix} \quad \mathbf{F}_c^4 = \begin{bmatrix} 0.82 & 0.95 & 0.4 \\ 0 & 0.35 & 0.9 \\ 0 & 0 & 0.3 \end{bmatrix}$$

$$\mathbf{G}_c^1 = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \quad \mathbf{G}_c^2 = \begin{bmatrix} 1 & 0 & 0.9 & 1 \\ 0.9 & 1 & 0 & 1 \\ 0 & 0.9 & 1 & 0.9 \end{bmatrix} \quad \mathbf{G}_c^3 = \begin{bmatrix} 0.9 & 0 & 0.8 & 1 \\ 0.9 & 1 & 0 & 0.9 \\ 0 & 0.8 & 1 & 0.8 \end{bmatrix} \quad \mathbf{G}_c^4 = \begin{bmatrix} 0.8 & 0 & 1 & 0.9 \\ 0.8 & 1 & 0 & 0.8 \\ 0 & 0.9 & 1 & 0.8 \end{bmatrix}$$

$$\zeta_c^1 = \begin{bmatrix} 0.4 & 0 & 0 \\ 0 & 0.5 & 0 \\ 0 & 0 & 0.3 \end{bmatrix} \quad \zeta_c^2 = \begin{bmatrix} 0.3 & 0 & 0 \\ 0 & 0.4 & 0 \\ 0 & 0 & 0.5 \end{bmatrix} \quad \zeta_c^3 = \begin{bmatrix} 0.5 & 0 & 0 \\ 0 & 0.3 & 0 \\ 0 & 0 & 0.4 \end{bmatrix} \quad \zeta_c^4 = \begin{bmatrix} 0.3 & 0 & 0 \\ 0 & 0.5 & 0 \\ 0 & 0 & 0.4 \end{bmatrix}$$

$$\mathbf{H}_c^1 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \mathbf{H}_c^2 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \mathbf{H}_c^3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \quad \mathbf{H}_c^4 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

The above matrices have no physical significance and were selected to ensure stability and observability. The calculations from the ith processor are represented by state vector $\mathbf{x}_c^i(k)$; the corresponding state transition matrix is given by $\mathbf{F}_c^i$. The input to each channel is $\mathbf{Y}_{\text{in}}^i(k)$ with input matrix $\mathbf{G}_c^i$. The form of the input $\mathbf{Y}_{\text{in}}^i(k)$ is

$$\mathbf{Y}_{\text{in}}^i(k) = [y_{\text{in}_i}(k)] = [\sin(2.4k)\ \ \cos(2.4k)\ \ \sin(1.4k)\ \ \cos(1.4k)] \qquad (i = 1, 2, 3, 4)$$

The process noise for each channel is represented by zero-mean white Gaussian noise $\mathbf{w}_c^i(k)$ and noise matrix $\zeta_c^i(k)$. The measurement matrix for each channel is $\mathbf{H}_c^i$, and the zero-mean white Gaussian measurement noise is $\mathbf{v}_c^i(k)$. The assumption is made that $\mathbf{w}_c^i(k)$ and $\mathbf{v}_c^i(k)$ are independent with covariances $\mathbf{Q}_c^i$ and $\mathbf{R}_c^i$, respectively. For this example,

$$\mathbf{Q}_c^i(k) = \begin{bmatrix} 0.5 & 0 & 0 \\ 0 & 0.5 & 0 \\ 0 & 0 & 0.5 \end{bmatrix} \qquad \mathbf{R}_c^i(k) = \begin{bmatrix} 0.7 & 0 & 0 \\ 0 & 0.7 & 0 \\ 0 & 0 & 0.7 \end{bmatrix} \qquad (i = 1, 2, 3, 4)$$

After 10 iterations in the simulation of the calculation process, a perturbation occurs such that the matrix $\mathbf{F}_c^i$ for each channel is changed to the transpose $[\mathbf{F}_c^i]^T$, thus yielding an incorrect calculation.

Detecting that a perturbation has occurred using Kalman filtering, statistical decision theory, and data fusion is desired.

The Kalman filters are implemented in Prediction-Correction Form (ref. 5) and estimate the calculated command vector of each processor. Thus, for a predicted state estimate,

$$\widehat{\mathbf{x}}_c^i(k|k-1) = \mathbf{F}_c^i(k)\,\widehat{\mathbf{x}}_c(k-1|k-1) + \mathbf{G}_c^i(k)\ \mathbf{z}_{\mathrm{in}}^i(k) \tag{15}$$

the predicted error covariance is

$$\mathbf{P}_c^i(k|k-1) = \mathbf{F}_c^i(k)\,\mathbf{P}_c^i(k-1|k-1)\ [\mathbf{F}_c^i(k)]^T + \zeta_c^i(k)\ \mathbf{Q}_c^i(k)\ [\zeta_c^i(k)]^T \tag{16}$$

The filter gain is

$$\mathbf{K}_c^i(k) = \mathbf{P}_c^i(k|k-1)\ [\mathbf{H}_c^i(k)]^T \{\mathbf{H}_c^i(k)\ \mathbf{P}_c^i(k|k-1)\ [\mathbf{H}_c^i(k)]^T + \mathbf{R}_c^i(k)\}^{-1} \tag{17}$$

For the updated state estimate,

$$\widehat{\mathbf{x}}_c^i(k|k) = \widehat{\mathbf{x}}_c^i(k|k-1) + \mathbf{K}_c^i(k)[\mathbf{z}_c^i(k)\ \ - \mathbf{H}_c^i(k)\ \widehat{\mathbf{x}}_c^i(k|k-1)] \tag{18}$$

the updated error covariance is

$$\mathbf{P}_c^i(k|k) = [\mathbf{I} - \mathbf{K}_c^i(k)\ \mathbf{H}_c^i(k)]\ \mathbf{P}_c^i(k|k-1) \tag{19}$$

The state estimation errors for each of the four Kalman filters are shown in figure 7. Note that once the Kalman filters have reached steady state, the estimation errors are 0 until the state transition matrices are changed at 10 iterations.

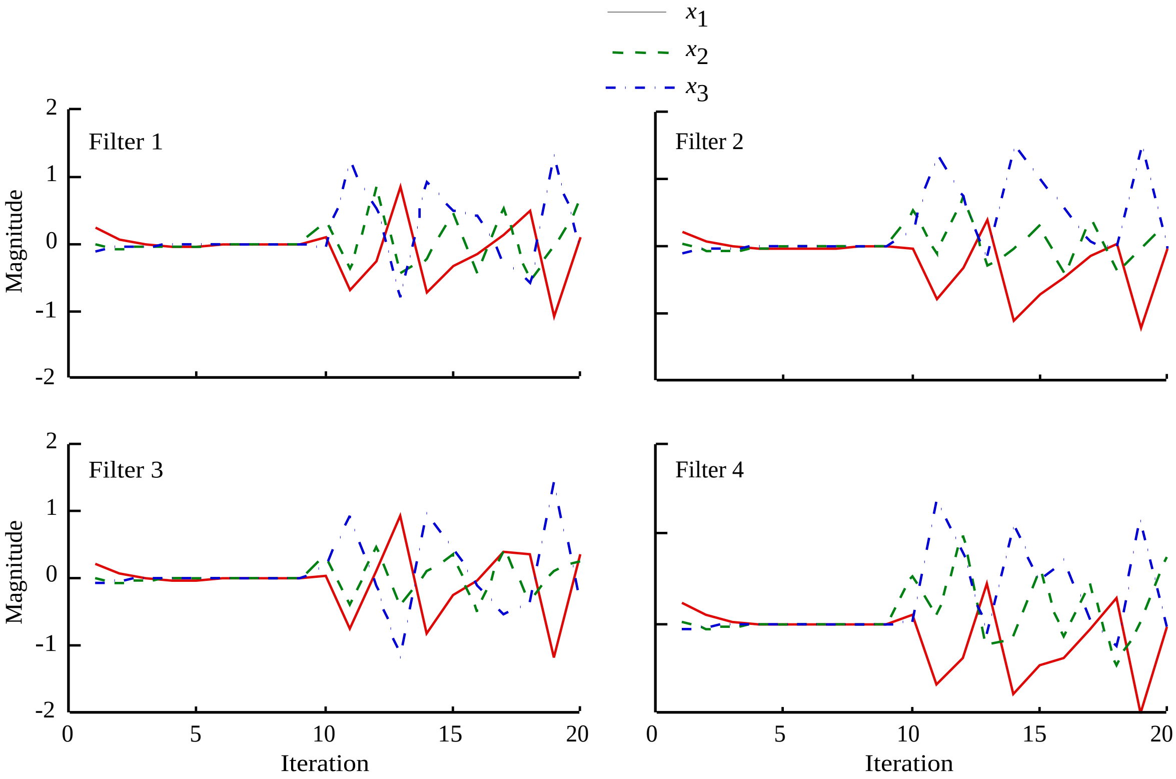

Figure 7. State estimation errors for the four Kalman filters of the example.

The residual for each channel is the absolute value of the innovations sequence, which is the bracketed term in equation (18). Thus, the residual vector is given by

$$\mathbf{r}_c^i(k) = [r_{c_j}^i] = |\mathbf{z}_c^i(k) - \mathbf{H}_c^i(k)\ \hat{\mathbf{x}}_c^i(k|k-1)| \qquad (j = 1, 2, 3) \tag{20}$$

The innovations sequence is a white random sequence whose mean (μ_c^i) is 0 if the calculations are correct. A Bayesian decision rule (ref. 6) will be used in this example for each calculation of each channel. The hypotheses for the decision rule for the jth calculation of the ith processor are given by

$$\left.\begin{array}{lll} H1^i_{c_j} : r^i_{c_j}(k) = \mu^i_{c_j} + v^i_{c_j}(k) & \rightarrow \text{ Incorrect calculation} & (\text{Mean } = \mu^i_{c_j} \neq 0) \\ H0^i_{c_j} : r^i_{c_j}(k) = v^i_{c_j}(k) & \rightarrow \text{ Correct calculation} & (\text{Mean } = \mu^i_{c_j} = 0) \end{array}\right\} \tag{21}$$

For this example, the *a priori* probabilities for these hypotheses are 0.5. The decision rule for the Gaussian case assuming unity variance is given by

$$r^i_{c_j} \underset{H0^i_{c_j}}{\overset{H1^i_{c_j}}{\gtrless}} + \frac{\mu^i_{c_j}}{2} + \frac{1}{\mu^i_{c_j}} \ln \left\{ \frac{P(H0_{c_j})[C10_{c_j} - C00_{c_j}]}{[1 - P(H0_{c_j})][C01_{c_j} - C11_{c_j}]} \right\} \tag{22}$$

The left-hand side of equation (22) is the residual given in equation (20), and the right-hand side of equation (22) is the threshold for the decision process. The threshold is dependent on the mean of the residual, the *a priori* probabilities of the hypotheses given in equations (21), and the costs associated with the decision process. The term $C\alpha\beta_{c_j}$ is the cost of deciding, for the jth calculation, that α is true when β is actually true. If the residual is less than the threshold, then hypothesis $H0^i_{c_j}$ of equations (21) is accepted and the calculation is considered correct. Otherwise, hypothesis $H1^i_{c_j}$ is accepted and the calculation is considered incorrect. For this example, the costs of making a correct decision (i.e., $\alpha = \beta$) are all 0, and the costs of making an incorrect decision (i.e., $\alpha \neq \beta$) are all 0.5. The performance of the Bayesian detectors for each channel, in terms of the probability of false alarm and the probability of miss, is given, respectively, by

$$Pfa^i_{c_j} = P(D1^i_{c_j}|H0^i_{c_j}) = \frac{1}{\sqrt{2\pi}} \int_{\lambda^i_{c_j}}^{\infty} e^{-(r^i_{c_j})^2/2}\ dr^i_{c_j} \tag{23}$$

and

$$Pm^i_{c_j} = P(D0^i_{c_j}|H1^i_{c_j}) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\lambda^i_{c_j}} e^{-(r^i_{c_j}-\mu^i_{c_j})^2/2}\ dr^i_{c_j} \tag{24}$$

For this example, the residuals are the innovations sequence defined in equation (20), and the means $\mu^i_{c_j}$ are unity. The integral limit $\lambda^i_{c_j}$ is defined to be the threshold given as the right-hand side of equation (22).

The error decisions for the three calculations of the state vector from processor 1 are shown in figure 8. In these plots, a value of 0 means that the decision process had not yet begun because the Kalman filters were being initialized. A value of −1 indicates that the calculation is correct, and a value of +1 indicates that the calculation is incorrect. For each calculation, all residuals were larger than the thresholds after 10 iterations, and thus the three calculations were considered incorrect. This decision is reflected in each of the three plots by the transition from −1 to +1. The error decision plots for the calculations of processors 2, 3, and 4 are analogous to figure 8. The probabilities of a missed detection and false alarm for the local decisions of each processor are 0.3083 and 0.0665, respectively.

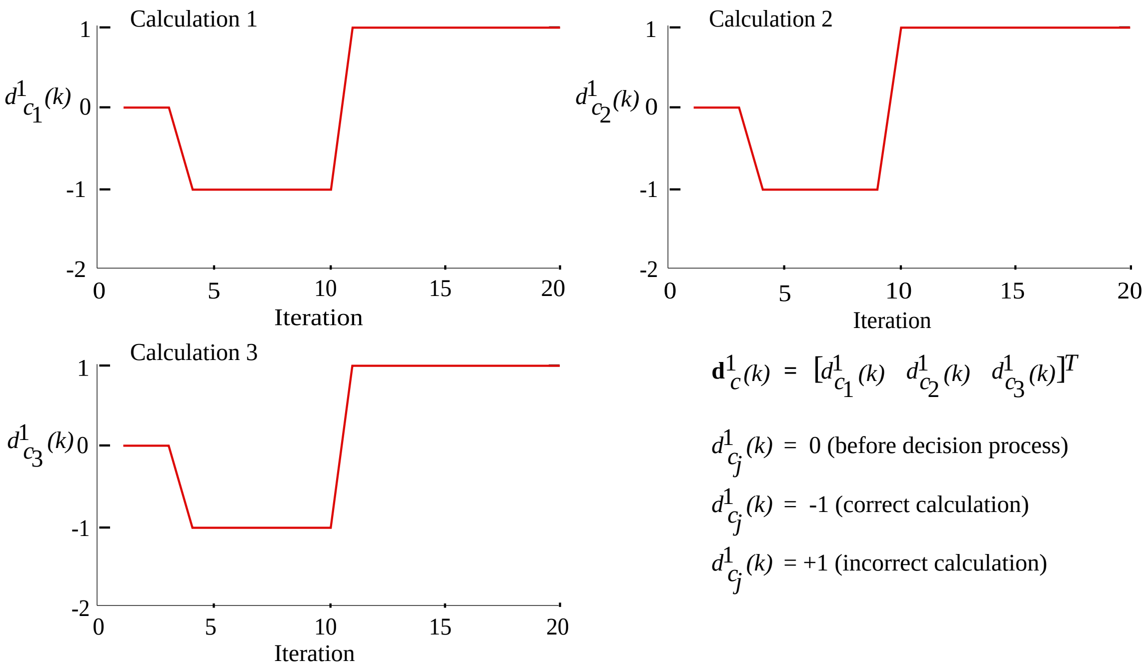

Figure 8. Error decisions for each calculation of the state vector from processor 1.

The fusion hypotheses for each processor are given by

$H1^i_c$: Incorrect command calculations of ith processor

$H0^i_c$: Correct command calculations of ith processor

The *a priori* probabilities for these hypotheses are 0.5 for this example. The fusion rule (ref. 7) for the local decisions from each processor is given by

$$d^i_c(k) = f[d^i_{c_j}(k)] = \left\{ \begin{array}{lll} 1 & \rightarrow \; H1^i_c & (a^{0^i}_c + \sum_{j=1}^{n} a^i_{c_j} \; d^i_{c_j}(k) > 0) \\ -1 & \rightarrow \; H0^i_c & (\text{otherwise}) \end{array} \right\} \tag{25}$$

where

$$\mathbf{d}^i_c(k) = [d^i_{c_j}(k)] \qquad a^{0^i}_c = \ln \frac{P(H1^i_c)}{P(H0^i_c)} \qquad a^i_{c_j} = \left\{ \begin{array}{ll} \ln \dfrac{1 - Pm^i_{c_j}}{Pfa^i_{c_j}} & (d^i_{c_j}(k) = 1) \\ \ln \dfrac{1 - Pfa^i_{c_j}}{Pm^i_{c_j}} & (d^i_{c_j}(k) = -1) \end{array} \right.$$

The optimal fusion rule of reference 7 shown in equation (25) is a weighted sum of the local decisions for each processor. The weights are based on the performance of the local detectors. The performance of this fusion process for each processor, assuming equal local noise covariances, was given in reference 4 to be

$$PF^i_c = \sum_{j=0}^{3} \binom{3}{j} (Pfa^i_c)^j (1 - Pfa^i_c)^{3-j} \, u[A^{0^i}_c + a^i_c(2j - 3)] \tag{26}$$

$$PM_c^i = \sum_{j=0}^{3} \binom{3}{j} (1 - Pm_c^i)^j (Pm_c^i)^{3-j} \; u[A_c^{0^i} + a_c^i(3 - 2j)] \tag{27}$$

where

$$A_c^{0^i} = \ln \frac{P(H1_c^i)}{P(H0_c^i)} + \frac{3}{2} \ln \frac{Pm_c^i(1 - Pm_c^i)}{Pfa_c^i(1 - Pfa_c^i)} \qquad\qquad a_c^i = \frac{3}{2}\left[\ln \frac{1 - Pm_c^i}{Pfa_c^i} + \ln \frac{1 - Pfa_c^i}{Pm_c^i}\right]$$

with

$$u[\cdot] = \text{Unit step function} \qquad Pm_c^i = Pm_{c_1}^i = Pm_{c_2}^i = Pm_{c_3}^i \qquad Pfa_c^i = Pfa_{c_1}^i = Pfa_{c_2}^i = Pfa_{c_3}^i$$

The fused error decision for the calculations of processor 1 is shown in figure 9. Note that figure 9 shows the plot of the error decision that results from the fusion of the three error decisions for the calculations of processor 1, as shown in figure 8. The fused error decision of figure 9 indicates the decision that the calculations of processor 1 are incorrect after iteration 10. The fused error decisions for the calculations of processors 2–4 were essentially identical to those of processor 1 shown in figure 9. The probabilities of a missed detection and false alarm for the fused decisions of each processor are 0.2265 and 0.0127, respectively.

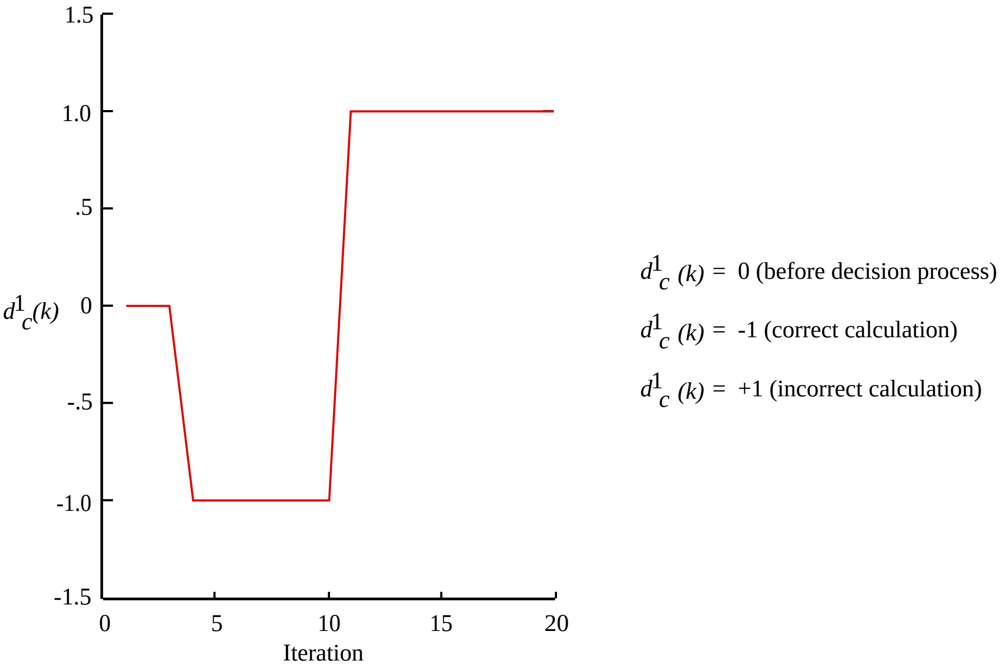

Figure 9. Fused error decision for local error decisions for processor 1.

The hypotheses for the fused decision process for global command calculations are given by

$$\left.\begin{array}{l} H1_c\text{: Incorrect calculation} \\[1em] H0_c\text{: Correct calculation} \end{array}\right\} \tag{28}$$

For this example, the *a priori* probabilities for these hypotheses are 0.5. The fused decision process for global command calculations is given by the same algorithm of reference 7 and is

$$d_c(k) = f[d_c^i(k)] = \left\{ \begin{array}{llll} 1 & \rightarrow & H1_c & (a_c^0 + \sum_{i=1}^{4} a_c^i \; d_c^i(k) > 0) \\ -1 & \rightarrow & H0_c & (\text{otherwise}) \end{array} \right\} \tag{29}$$

where

$$a_c^0 = \ln \frac{P(H1_c)}{P(H0_c)} \qquad a_c^i = \left\{ \begin{array}{ll} \ln \frac{1 - PM_c^i}{PF_c^i} & (d_c^i(k) = 1) \\ \ln \frac{1 - PF_c^i}{PM_c^i} & (d_c^i(k) = -1) \end{array} \right.$$

The performance of this global fusion process is given by

$$PF_c = \sum_{i=1}^{4} \binom{4}{i} (PF_c^i)^i (1 - PF_c^i)^{4-i} \, u[A_c^0 + a_c(2i - 4)] \tag{30}$$

$$PM_c = \sum_{i=1}^{4} \binom{4}{1} (1 - PM_c^i)^i (PM_c^i)^{4-i} \, u[A_c^0 + a_c(4 - 2i)] \tag{31}$$

where

$$A_c^0 = \ln \frac{P(H1_c)}{P(H0_c)} + 2 \ln \frac{PM_c(1 - PM_c)}{PF_c(1 - PF_c)} \qquad a_c = 2 \left[\ln \frac{(1 - PM_c)}{PF_c} + \ln \frac{(1 - PF_c)}{PM_c} \right]$$

with

$$u[\cdot] = \text{Unit step function} \quad PM_c = PM_c^1 = PM_c^2 = PM_c^3 = PM_c^4 \quad PF_c = PF_c^1 = PF_c^2 = PF_c^3 = PF_c^4$$

The global error decision that results from the fusion of the error decisions for processors 1–4 is shown in figure 10. The plot indicates that after 10 iterations, calculations made by the four-channel system are considered incorrect. The global probabilities of a missed detection and false alarm are 0.2228 and 0.000948, respectively.

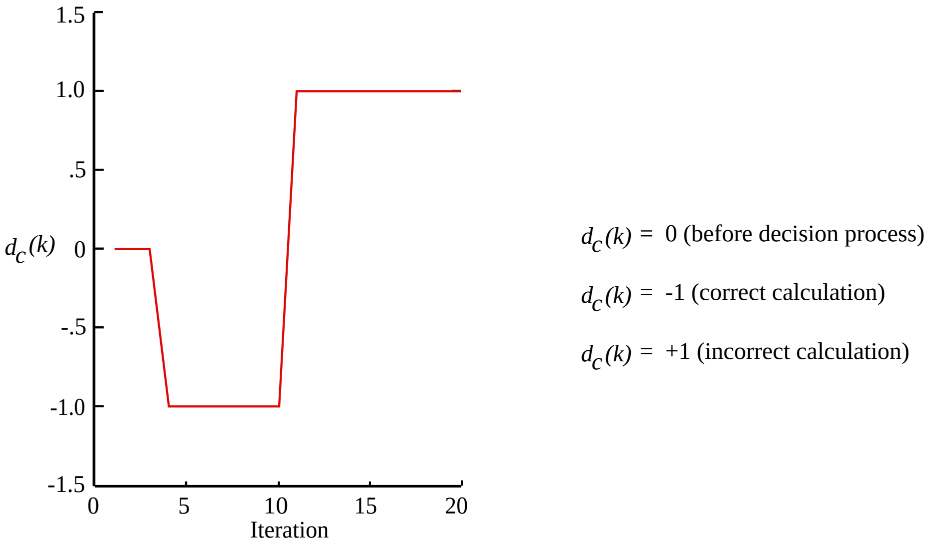

Figure 10. Global error decision for calculations in a four-channel system.

Concluding Remarks

A strategy has been presented for dynamically monitoring digital controllers in the laboratory for susceptibility to electromagnetic disturbances. In particular, this paper discusses the use of Kalman filtering, data fusion, and decision theory in monitoring a given digital controller for control calculation errors. In this strategy, the control laws calculated in the digital controller were modeled as linear (or linearized) recursive state equations. This model was used in the design of Kalman filters that estimate the correct control calculations. The estimates of the correct control calculations were compared with the calculations obtained by the control computer. Residuals were then generated and used in probabilistic decision rules to determine if the calculations performed by the control unit were faulty. A decision was made for the command calculation of each control loop and these local decisions were weighted and fused into an integrity decision for control calculations by using an optimal fusion rule.

An example of this process was presented which can be used as a baseline design for future work. Future work includes an analysis of the baseline design for detection sensitivity to changes in matrix parameter values. Designs of the statistical decision rules, data fusion algorithms, and Kalman filter gains can be performed to optimize trade-offs such as sensitivity and diagnostic capability versus complexity, reliable detection without false alarms, and sensitivity to erroneous parameter changes with robustness to modeling errors.

NASA Langley Research Center
Hampton, VA 23681-0001
August 26, 1992

References

1. Belcastro, Celeste M.: *Laboratory Test Methodology for Evaluating the Effects of Electromagnetic Disturbances on Fault-Tolerant Control Systems.* NASA TM-101665, 1989.

2. DeLaat, John C.; and Merrill, Walter C.: *Advanced Detection, Isolation, and Accommodation of Sensor Failures in Turbofan Engines—Real-Time Microcomputer Implementation.* NASA TP-2925, 1990.

3. Bundick, W. Thomas: *Development of an Adaptive Failure-Detection and Identification System for Detecting Aircraft Control-Element Failures.* NASA TP-3051, 1991.

4. Belcastro, Celeste M.; Fischl, Robert; and Kam, Moshe: Fusion Techniques Using Distributed Kalman Filtering for Detecting Changes in Systems. *Proceedings of the 1991 American Control Conference, Volume 3,* IEEE Catalog No. 91CH2939-7, American Automatic Control Council, 1991, pp. 2296–2298.

5. Anderson, Brian D. O.; and Moore, John B.: *Optimal Filtering.* Prentice-Hall, Inc., c.1979.

6. Van Trees, Harry L.: *Detection, Estimation, and Modulation Theory. Part I—Detection, Estimation, and Linear Modulation Theory.* John Wiley & Sons, Inc., c.1968.

7. Chair, Z.; and Varshney, P. K.: Optimal Data Fusion in Multiple Sensor Detection Systems. *IEEE Trans. Aerosp. & Electron. Syst.,* vol. AES-22, no. 1, Jan. 1986, pp. 98–101.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY *(Leave blank)*

2. REPORT DATE
October 1992

3. REPORT TYPE AND DATES COVERED
Technical Memorandum

4. TITLE AND SUBTITLE
A Monitor for the Laboratory Evaluation of Control Integrity in Digital Control Systems Operating in Harsh Electromagnetic Environments

5. FUNDING NUMBERS
WU 505-64-10-10

6. AUTHOR(S)
Celeste M. Belcastro, Robert Fischl, and Moshe Kam

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
NASA Langley Research Center
Hampton, VA 23681-0001

8. PERFORMING ORGANIZATION REPORT NUMBER
L-17057

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
National Aeronautics and Space Administration
Washington, DC 20546-0001

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
NASA TM-4402

11. SUPPLEMENTARY NOTES
Belcastro: Langley Research Center, Hampton, VA; Fischl and Kam: Drexel University, Philadelphia, PA.

12a. DISTRIBUTION/AVAILABILITY STATEMENT

Unclassified–Unlimited

Subject Categories 08, 66, 33

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

This paper presents a strategy for dynamically monitoring digital controllers in the laboratory for susceptibility to electromagnetic disturbances that compromise control integrity. The integrity of digital control systems operating in harsh electromagnetic environments can be compromised by upsets caused by induced transient electrical signals. Digital system upset is a functional error mode that involves no component damage, can occur simultaneously in all channels of a redundant control computer, and is software dependent. The motivation for this work is the need to develop tools and techniques that can be used in the laboratory to validate and/or certify critical aircraft controllers operating in electromagnetically adverse environments that result from lightning, high-intensity radiated fields (HIRF), and nuclear electromagnetic pulses (NEMP). The detection strategy presented in this paper provides dynamic monitoring of a given control computer for degraded functional integrity resulting from redundancy management errors, control calculation errors, and control correctness/effectiveness errors. In particular, this paper discusses the use of Kalman filtering, data fusion, and statistical decision theory in monitoring a given digital controller for control calculation errors.

14. SUBJECT TERMS
Fault detection; Kalman filtering; Statistical decision theory; Electromagnetic disturbances; Digital controllers

15. NUMBER OF PAGES
21

16. PRICE CODE
A03

17. SECURITY CLASSIFICATION OF REPORT
Unclassified

18. SECURITY CLASSIFICATION OF THIS PAGE
Unclassified

19. SECURITY CLASSIFICATION OF ABSTRACT

20. LIMITATION OF ABSTRACT

NASA-Langley, 1993